What is claimed is:

1. A method for generating an encryption key for use with a host device having a host identification stored therein, the method comprising:

retrieving the host identification from the host device;

generating at least one content variable;

combining the host identification and the at least one content variable to produce two or more combinations, wherein the method used to combine the host identification and the at least one content variable repeatedly produces the same two or more combinations; and

coalescing the two or more combinations to produce the encryption key, wherein the method of coalescing the two or more combinations repeatedly produces the same encryption key.

2. The encryption key generation method of claim 1 wherein coalescing the two combinations comprises:

concatenating the two or more combinations using a predetermined method, wherein concatenating the two or more combinations repeatedly produces the same encryption key.

3. The method of claim 1, wherein the host device includes a secure clock, the method further comprising:

obtaining a time variable from the secure clock within the host device;

combining the host identification, the at least one content variable and the time variable to produce a plurality of different combinations, wherein the method

used to combine the host identification, the at least one content variable and the time variable repeatedly produces the same plurality of different combinations; and

coalescing the plurality of different combinations to produce the encryption key, wherein the method of coalescing the plurality of different combinations repeatedly produces the same encryption key.

4. A method for generating an encryption key to encrypt a block of plaintext for use with a host device having a secure clock and a host identification assigned thereto and saved therein, the method comprising:

retrieving the host identification from the host device;

generating a content identification, wherein the content identification corresponds to the block of plaintext;

obtaining a time variable from the secure clock within the host device;

combining the host identification, the content identification and the time variable to produce at least six combinations thereof; and

coalescing the at least six combinations to generate the encryption key, wherein the method of coalescing the at least six combinations repeatedly produces the same encryption key.

5. A method for encrypting a block of plaintext for transmission over an unsecured interface to a storage device, for use with a host device having a host identification assigned thereto and stored therein, the method comprising:

retrieving the host identification from the host device;

generating at least one content variable;

combining the host identification and the at least one content variable to produce two or more combinations, wherein the method used to combine the host identification and the at least one content variable repeatedly produces the same two or more combinations;

coalescing the two or more combinations to produce a first encryption key, wherein the method of coalescing the two or more combinations repeatedly produces the same first encryption key;

encrypting the block of plaintext using the first encryption key to produce a block of ciphertext;

appending the at least one content variable to the block of ciphertext;

transmitting the block of ciphertext and the appended at least one content variable over the unsecured interface to the storage device; and

storing the block of ciphertext and the appended one or more content variables within the storage device.

6. The method of encrypting the block of plaintext of claim 5, wherein the host device further comprises a secure clock, the method further comprising:

obtaining a first time variable from the secure clock within the host device;

combining the host identification, the at least one content variable and the first time variable to produce a first plurality of different combinations, wherein the method used to combine the host identification, the at least one content variable and the first time variable repeatedly produces the same first plurality of different combinations; and

coalescing the first plurality of different combinations to produce the first encryption key, wherein the method of coalescing the first plurality of combinations repeatedly produces the same first encryption key.

7. The method of encrypting the block of plaintext of claim 6, for further use decrypting the block of ciphertext, the method comprising:

retrieving the stored block of ciphertext and the appended at least one content variable from the storage device;

retrieving the host identification from the host device;

obtaining a second time variable from the secure clock within the host device;

combining the host identification, the at least one content variable and the second time variable to produce a second plurality of different combinations; and

coalescing the second plurality of different combinations to produce a second encryption key, wherein if the first time variable and the second time variable do not match, the second encryption key will not decrypt the block of ciphertext and if the first time variable matches the second time variable the second encryption key will decipher the block of ciphertext.

8. The method of encrypting the block of plaintext of claim 5 for further use decrypting the stored block of ciphertext, the method comprising:

retrieving the stored block of ciphertext and the appended at least one content variable from the storage device;

retrieving the host identification from the host device;

combining the host identification and the at least one content variables to produce two or more combinations;

coalescing the two or more combinations to produce the encryption key; and

decrypting the block of ciphertext with the encryption key to produce the block of plaintext.